

CRIMINAL JUSTICE USER AGREEMENT

This Agreement, is entered into between the Florida Department of Law Enforcement (hereinafter referred to as FDLE), an agency of the State of Florida with headquarters at 2331 Phillips Road, Tallahassee, Florida and the

_____ with headquarters at

_____ (hereinafter referred to as the User).

Whereas, FDLE is authorized by law to operate and regulate the Criminal Justice Network (hereinafter CJNet) as an intra-agency information and data-sharing network for use by the state's criminal justice agencies;

Whereas, FDLE is authorized by law to establish and operate the Florida Crime Information Center (hereinafter FCIC) for the exchange of information relating to crimes, criminals and criminal activity;

Whereas, FDLE participates in the National Crime Information Center (hereinafter NCIC), a service of the United States Department of Justice, the Interstate Identification Index (hereinafter III), and the National Law Enforcement Telecommunication System (hereinafter NLETS), and serves as Florida's Criminal Justice Information Services (CJIS) Systems Agency (CSA) for the interstate transmission of criminal justice information to and from agencies in Florida and agencies in the continental United States, Alaska, Hawaii, U.S. Virgin Islands, Canada and Puerto Rico;

Whereas, the User requires access to intrastate and interstate criminal justice information systems provided by FDLE through the CJNet in order to effectively discharge its public duties;

Whereas, FDLE will facilitate local law enforcement and other criminal justice agencies' requests to participate in the information services provided on CJNet, provided the User agrees to abide by applicable federal and state laws; administrative code, and all policies, procedures and regulations related to these systems. FDLE retains full control over the management and operation of CJNet and FCIC.

Therefore, in consideration of the mutual benefits to be derived from this Agreement, the FDLE and the User do hereby agree as follows:

(This User agreement is designed for use with all Florida criminal justice agencies. If your agency does not perform a specific function, the provisions regarding that function will not apply to your agency.)

SECTION I FCIC/NCIC/CJNET FDLE REQUIREMENTS

FDLE is duly authorized and agrees to ensure access to the information services provided on CJNet and adhere to the following:

1. Serve as the CSA for the State of Florida and provide the User with access to criminal justice information as is available in the FCIC/NCIC and III systems and NLETS through CJNet, and to serve as the means of exchanging criminal justice information between the User and other criminal justice agencies on CJNet.
2. Provide the opportunity for CJIS certification/re-certification training.
3. Provide the User with information concerning privacy and security requirements imposed by state and federal laws, rules and regulations.
4. Provide state criminal history record check services for non-criminal justice purposes as provided by law.
5. Act as the central state repository; provide identification, record keeping, and exchange of criminal history record information services.
6. Facilitate access, using CJNet, to other information applications or systems that the User may be authorized to access.

SECTION II FCIC/NCIC/CJNET USER REQUIREMENTS

By accepting access as set forth above, the User agrees to adhere to the following to ensure continuation of access:

1. **USE OF THE SYSTEM:** Use of the CJNet and any system accessed via the CJNet is restricted to the administration of criminal justice or as otherwise specifically authorized or required by statute. Information obtained from the FCIC/NCIC files, or computer interfaces to other state or federal systems, by means of access granted through CJNet, can only be used for authorized purposes in compliance with FCIC/NCIC and III rules, regulations and operating procedures, and state and federal law. It is the responsibility of the User to insure access to CJNet is for authorized purposes only, and to regulate proper use of the network and information at all times. Users must establish appropriate written standards, which may be incorporated with existing codes of conduct, for disciplining violators of this and any incorporated policy.

Users that provide an interface between FDLE and other criminal justice agencies must abide by all of the provisions of this agreement. Agencies that access FDLE systems by interfacing through other agencies must, likewise, abide by all provisions of this agreement. An Interagency User Agreement is required when access to CJNet is provided by the User to another agency.

- a. **MESSAGES:** Only law enforcement and other criminal justice messages shall be sent over and through the CJNet. All messages will be treated as privileged unless otherwise indicated. User should make prudent use of regional and statewide broadcast message requests. All messages must use plain English text in the message.
- b. **COMPLIANCE:** Access FCIC/NCIC and other CJNet applications in strict compliance with applicable CJNet, FCIC, NCIC, III and NLETS policies including, but not limited to, policies, practices and procedures relating to:
 - i) **TIMELINESS:** FCIC/NCIC records must be entered, modified, cleared, and canceled promptly in order to ensure system accuracy and effectiveness. Users that perform FCIC/NCIC updates for other agencies must comply with timeliness requirements for the records entered for the serviced agencies as well.
 - ii) **HOT FILE ENTRIES:** User agencies that have personnel dedicated to maintain a 24-hour, seven-day a week FCIC/NCIC operation will be allowed to make entries into the FCIC/NCIC Hot Files.
 - (a) Users making entries for another law enforcement agency must execute an Interagency Agreement outlining each agency's responsibilities.
 - (b) Certain categories of FCIC Hot File records will be made available to the public on the Internet via the FCIC Public Access System (PAS), unless explicitly flagged by the entering agency for exclusion.
 - iii) **QUALITY ASSURANCE:** Appropriate and reasonable quality assurance procedures must be in place, including second party verification during entry, to ensure all entries in FCIC/NCIC are complete, accurate, and valid.
 - iv) **VALIDATION:** The User must validate all records that the User has entered into the system for accuracy and retention. To be in compliance with FCIC/NCIC rules, regulations and operating procedures, the User must ensure each record is modified to confirm the successful validation of each record on file in FCIC/NCIC. Failure to modify a record to indicate validation may result in its removal from the file. Users that make entries into the FCIC/NCIC Hot Files are responsible for maintaining written validation procedures.
 - v) **HIT CONFIRMATION:** The User must comply with FCIC/NCIC rules, regulations and operating procedures by responding to the hit

confirmations in a timely manner (within ten minutes or one-hour depending on priority).

- vi) **DISSEMINATION:** Information obtained from the FCIC/NCIC hot files, CJNet or computer interfaces to other state or federal systems, by means of access granted pursuant to Section 943.0525, F.S., can only be used for official criminal justice purposes.

Compliance with Chapter 119, F.S., is accomplished by directing record requests to FDLE per Chapter 11C-6, F.A.C., and section 943.053(3), F.S. It is the responsibility of the authorized User agency to ensure that access to the CJNet is for authorized criminal justice purposes only, and to regulate proper access to and use of the network and information at all times.

The User will disseminate criminal history record information derived from federal records or systems only to criminal justice agencies and only for criminal justice purposes. Criminal justice purposes include criminal justice employment screening.

- vii) **RETENTION:** Criminal history records, whether retrieved from III or the state system, which an agency maintains, must be kept in a secure records environment to prevent unauthorized access.
- (a) Retention of criminal history records, whether retrieved from III or the state system, for extended periods should only be considered when the time sensitivity of the specific record is important.
- (b) When retention of criminal history records, whether retrieved from III or the state system, is no longer required, final disposition will be accomplished in a secure manner in compliance with state law, FCIC/NCIC and III rules, regulations and operating procedures to preclude unauthorized access.
- viii) **CRIMINAL HISTORY TRANSMISSION:** Any electronic device that uses wireless or radio technology to transmit voice data may be used for the transmission of criminal history record information only when an officer determines there is an immediate need for this information to further an investigation or there is a situation affecting the safety of an officer or the public.

A facsimile machine may be used to transmit criminal history information between criminal justice agencies, provided both agencies have an NCIC Originating Agency Identifier (ORI) and are authorized to receive criminal history information. Appropriate measures must be taken to prevent unauthorized viewing or receipt by unauthorized persons

- ix) **LOGGING:** Each interface agency accessing FCIC/NCIC Hot File and III systems shall ensure that an automated log is maintained. The Hot File portion of this log must be maintained for a minimum of six months, and the III portion must be maintained for a minimum of four years.
- (a) Automated logging is a feature included in the application software provided by FDLE, and local agencies are encouraged to retain these logs for future reference. Users purchasing or developing an interface to FCIC must ensure logging is an included feature.
 - (b) The automated transaction log must identify: the operator on all transactions, the agency authorizing all transactions, the requester and secondary recipient for all criminal history transactions. This information can be captured at log-on and can be a name, badge number, serial number, or other **unique** identifier.
 - (c) The User may only disseminate information to another authorized recipient and must maintain a record of any dissemination of state or federal criminal history information. This record will reflect at a minimum: (1) date of release; (2) to whom the information relates; (3) to whom the information was released; (4) the State Identification (SID) and/or the FBI number(s); and (5) the purpose for which the information was requested. The User must also be able to identify the reason for all III inquiries upon request from the FBI or FDLE.
- x) **INFORMATION ACCESS:** The User will allow only properly screened, authorized personnel performing a criminal justice function to have access to information contained within the CJNet, FCIC/NCIC or other state criminal justice information system files. The User will also provide assistance to other criminal justice agencies not equipped with direct FCIC access in compliance with FCIC/NCIC and III rules, regulations and operating procedures, but only to the extent that such assistance is not otherwise prohibited.
- xi) **WORKSTATION:** FDLE is not responsible for the workstation acquisition, maintenance, operation, repair, supplies or workstation operation personnel costs. The User must notify FDLE immediately, should an FCIC/NCIC workstation malfunction or become inoperable. All costs associated with returning the workstation to operation, other than CJNet costs, will be the User's responsibility. FDLE will assist with executing trouble-shooting procedures.

2. **AUDITS:** All agencies having access to CJNet, FCIC/NCIC and the III data shall permit an FDLE appointed inspection team to conduct inquiries with regard to any allegations or potential security violations, as well as for routine audits.

FDLE conducts regularly scheduled compliance and technical security audits of every agency accessing the CJNet to ensure network security, conformity with state law, and compliance with all applicable FDLE, CJNet, FCIC/NCIC and III rules, regulations and operating procedures. Compliance and technical security audits may be conducted at other than regularly scheduled times.

3. **TRAINING:** The User is responsible for complying with training requirements established in CJIS Security Policy and the rules, regulations, and policies established by FCIC/NCIC, III and FDLE. Each agency is responsible for remaining current in the applications, procedures, and policies and ensuring personnel attend these training sessions.
- a. Only operators who have successfully completed CJIS certification shall be allowed to have unsupervised access to the FCIC/NCIC system.
 - b. FCIC/NCIC operators who are in their initial six months of assignment may be permitted supervised access to FCIC/NCIC. Operators must successfully complete CJIS certification within six months of appointment or assignment to duties requiring direct access to FCIC/NCIC.
 - c. The User will require all personnel who access FCIC/NCIC to successfully complete CJIS Certification. The User agrees to remove from FCIC/NCIC access any employee who fails to achieve required certification standards, whose certification has expired, whose certificate is otherwise rescinded or as directed by FDLE.
 - d. The User will require all information technology personnel, including vendors, who in the course of their assigned criminal justice duties, maintain or support a system or network component that has direct access to FCIC/NCIC, to successfully complete CJIS certification.
 - e. The User will maintain certification records of all CJIS certified personnel in a current status.
4. **RELOCATION:** Should the User desire to relocate the data circuit(s) and/or equipment connected to CJNet, the User must provide FDLE written notice 90 days in advance of the projected move. All costs associated with the relocation of the equipment and the data circuit(s), including delays in work order dates, will be borne by User unless FDLE has funding to make changes without charge. The repair and cost of any damages resulting from such relocation will be the User's responsibility.

The User must also provide 90 days advance notice when requesting additional access to FCIC/CJNet.

5. **LIABILITY:** The User understands that the FDLE, its officers, and employees shall not be liable in any claim, demand, action, suit, or proceeding, including, but not limited to, any suit in law or in equity, for damages by reason of, or arising out of, any false arrest or imprisonment or for any loss, cost, expense or damages resulting from or arising out of the acts, omissions, or detrimental reliance of the personnel of the User in entering, removing, or relying upon information transmitted through CJNet or in the FCIC/NCIC and NLETS information systems.
6. **CRIMINAL HISTORY RECORDS:** FDLE is authorized to establish an intrastate automated fingerprint identification system (IAFIS) and an intrastate system for the communication of information relating to crimes, criminals and criminal activity.

To support the creation and maintenance of the criminal history files, the User, as appropriate, will:

- a. Provide for inclusion in criminal history records information systems, adult and juvenile criminal fingerprints on all felony arrests; adult criminal fingerprints on all misdemeanors and comparable ordinance violation arrests; and juvenile fingerprints on misdemeanor arrests specified at Section 943.051, F.S. The submission of other juvenile misdemeanor arrest fingerprints is optional.
- b. Provide security for criminal history record information and systems. Train personnel who receive, handle or have access to criminal history record information.
- c. Screen all personnel who will have direct access to criminal history record information and reject for employment personnel who have violated or appear unwilling or incapable of abiding by the requirements outlined in this agreement.
- d. Defer to FDLE on any determination as to what purposes qualify for criminal justice versus non-criminal justice designation, as well as with respect to other purposes that may be authorized by law.
- e. Pursuant to a signed interagency agreement as authorized by Florida Statutes and/or federal regulations, the User may share state criminal history record information. Dissemination of information requires compliance with all applicable statutes, FCIC/NCIC and III rules, regulations and operating procedures, including logging. Agencies must maintain confidentiality of such record information that is otherwise exempt from Section 119.07(1), F.S., as provided by law.

SECTION III SECURITY REQUIREMENTS

Each agency must ensure compliance with the FBI CJIS Security Policy and the rules, regulations, policies and procedures established for CJNet, FCIC/NCIC, III and NLETS, which include but are not limited to System Security, Personnel Security, Physical Security, User Authorization, Technical Security, Dissemination of Information Obtained from the Systems, and Destruction of Records. By accepting access as set forth above, the agency agrees to adhere to the following security policies in order to ensure continuation of that access:

1. **PERSONNEL BACKGROUND SCREENING and POLICY FOR DISCIPLINE:** The User is required to conduct a background investigation on all terminal operators, programmers, consultants, other persons employed or utilized to effectuate access to or initiate transmission of CJNet information, and custodial, support, and/or contractor personnel accessing workstation areas unescorted by authorized personnel. Good management practices dictate the investigation should be completed prior to employment, but must, at a minimum, be conducted within the first thirty (30) days of employment or assignment. The User may conduct a preliminary on-line criminal justice employment check.

Before the background is completed the following requirements must be met:

- a. The User must submit applicant fingerprints for positive comparison against the state and national criminal history and for searching of the Hot Files.
- b. If a record of any kind is found, the User will not permit the operator to have access to the FCIC/NCIC system nor access workstation areas. The User will formally notify the FDLE CJIS Systems Officer (CSO) indicating access will be delayed pending review of the criminal history.
- c. When identification of the applicant has been established by fingerprint comparison and the applicant appears to be a fugitive, have pending criminal charges; have an arrest history for a felony or serious misdemeanor; have been found guilty of, regardless of adjudication, or entered a plea of nolo contendere or guilty to any felony or serious misdemeanor; or to be under the supervision of the court, the User will refer the matter to the FDLE CSO for review.
- d. Applicants who have been found guilty of, regardless of adjudication, or entered a plea of nolo contendere or guilty to a felony, will generally be denied access to FCIC/NCIC. Access will also generally be denied to any person with pending charges or who is under court supervision in relation to a criminal offense. If a determination is made by FDLE that FCIC/NCIC access by the applicant would not be in the public interest, such access will be denied and the User agency will be notified in writing of the access denial.

- e. Each agency must have a written policy for discipline of personnel who access CJNet for purposes that are not authorized, disclose information to unauthorized individuals, or violate FCIC/NCIC or III rules, regulations or operating procedures.
2. **PHYSICAL SECURITY:** The User will determine the perimeter for the physical security of devices that access or provide access to CJNet. Access shall be limited as to allow completion of required duties. The User must have a written policy that ensures and implements security measures, secures devices that access FCIC/NCIC/CJNet and prevents unauthorized use or viewing of information on these devices. The use of screen blanking software with password protection is recommended for devices that access FCIC/NCIC when the operator may leave the computer unsupervised. FDLE reserves the right to object to equipment location, security measures, qualifications and number of personnel who will be accessing FCIC/NCIC and to suspend or withhold service until such matters are corrected to its reasonable satisfaction.
3. **ADMINISTRATIVE SECURITY:** Each agency utilizing information services provided through CJNet must designate individual agency contacts to assist the agency and FDLE with the information services covered by this agreement. Training for these positions is provided by FDLE, and the User must ensure that its designee is keenly aware of the duties and responsibilities of each respective position. The User is required to provide FDLE with up-to-date contact information.
 - a. **TERMINAL AGENCY COORDINATOR:** Agencies accessing the FCIC/NCIC system must designate a Terminal Agency Coordinator (TAC) to ensure compliance with FCIC/NCIC and III rules, regulations and operating procedures, and to facilitate communication between FDLE and the agency. The TAC must maintain a current CJIS Certification. TACs appointed after February 2005 must attend TAC training.
 - b. **INFORMATION SECURITY OFFICER:** Agencies accessing the FCIC/NCIC system and/or the CJNet, must designate an Information Security Officer (ISO) to ensure security of the FCIC/NCIC workstations, the connection to CJNet, and any access to the information services provided on CJNet to or by the User.
 - c. **CJNet POINT OF CONTACT:** Agencies accessing applications using Public Key Infrastructure (PKI) security certificates on CJNet must designate a Point of Contact (POC). The POC will receive and approve the issuance and revocation of PKI certificates for agency members.
 - d. **FCIC PUBLIC ACCESS SYSTEM (PAS) CONTACT:** Agencies making entries into the FCIC Hot Files must designate a PAS Contact. The PAS Contact is responsible for any follow-up activities deemed appropriate by the agency in response to tips resulting from the posting of records on the PAS.

4. TECHNICAL SECURITY

- a. **DIAL-UP SERVICES:** Establishing dial-up services to FCIC/NCIC and CJNet will be permitted provided the User establishes appropriate security measures to ensure compliance with all rules, regulations, procedures, and the FBI CJIS Security Policy.
 - b. **ENCRYPTION:** All FCIC/NCIC/III data transmitted over any public network segment must be encrypted as required by the FBI CJIS Security Policy. This requirement also applies to any private data circuit that is shared with non-criminal justice users and/or is not under the direct security control of a criminal justice agency.
 - c. **DOCUMENTATION OF NETWORK CONFIGURATION:** The User must maintain, in current status, and provide upon request by FDLE a complete topological drawing, which depicts the User's network configuration as connected to CJNet. This documentation must clearly indicate all network connections, service agencies and interfaces to other information systems.
 - d. **CJNET CONNECTIVITY:** The User will ensure only authorized criminal justice agencies or agencies authorized by FDLE are permitted access to the CJNet via the User's CJNet connection.
 - e. **VIRUS PROTECTION SOFTWARE:** The User must ensure all devices with connectivity to CJNet employ virus protection software and such software shall be maintained in accordance with the software vendor's published updates.
5. **COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY:** The User must have a written policy documenting the actions to be taken in response to a possible computer security incident. The policy should include identifying, reporting, investigating and recovery from computer security incidents. The User will immediately notify FDLE of any suspected compromise of the CJNet.
 6. **PENETRATION TESTING:** The User shall allow the FBI and/or FDLE to periodically test the ability to penetrate the CJNet through the external network connection or system.
 7. **SECURITY AUTHORITY:** All policies, procedures and operating instructions contained in the FBI CJIS Security Policy and FCIC/NCIC, III and NLETS documents, operating manuals and technical memoranda, are hereby incorporated into and made a part of this agreement, except to the extent that they are inconsistent herewith or legally superseded by higher authority.
 8. **CLIENT SOFTWARE LICENSE:** The FCIC II Client Software (eAgent) license from Diverse Computing, Incorporated is located in the Help menu of the eAgent

client software. The FCIC II Client Software (eAgent) license is made a part of and incorporated by reference into this User Agreement and shall be binding on the User upon acceptance of the software.

SECTION IV MISCELLANEOUS REQUIREMENTS

1. FDLE has received funding from the United States Department of Justice and is subject to and must demand intrastate users of its criminal history record services adhere to US Code (28 U.S.C. section 534), State Statute (Chapter 943 F.S.), Code of Federal Regulations (28 C.F.R. Part 20), Florida Administrative Code (Chapter 11C-6, F.A.C.), FCIC/NCIC and III rules, regulations and operating procedures which this agreement incorporates both present and future.
2. **PENALTIES AND LIABILITIES:** Any non-compliance with the terms of this Agreement concerning the use and dissemination of criminal history information may subject the User's officers or employees to a fine not to exceed \$10,000 as provided for in the Code of Federal Regulations, Title 28, Section 20.25, and/or discontinuance of service. Moreover, certain offenses against system security and the information contained therein are crimes under Florida Statutes and can result in criminal prosecution.
3. **PROVISIONS INCORPORATED:** The User shall be bound by applicable federal and state laws, federal regulations and the rules of FDLE to the same extent that the User would be if such provisions were fully set out herein. Moreover, this Agreement incorporates both present and future law, regulations and rules.
4. **TERMINATION:** Either party may terminate this Agreement, with or without cause, upon providing advanced written notice of 45 days. Termination for cause includes, but is not limited to, any change in the law that affects either party's ability to substantially perform as originally provided in this Agreement. Should the aforementioned circumstances arise, either party may terminate or modify the Agreement accordingly.

FDLE reserves the right to terminate service, without notice, upon presentation of reasonable and credible evidence that the User is violating this Agreement or any pertinent federal or state law, regulation or rule.
5. **MODIFICATIONS:** Modifications to the provisions in this Agreement shall be valid only through execution of a formal Agreement amendment.
6. **ACCOUNTABILITY:** To the extent provided by the laws of Florida, the User agrees to be responsible for the negligent acts or omissions of its personnel arising out of or involving any information contained in, received from, entered into or through CJNet, FCIC/NCIC, III and NLETS.

7. **ACKNOWLEDGEMENT:** The User hereby acknowledges the duties and responsibilities as set out in this Agreement. The User acknowledges that these duties and responsibilities have been developed and approved by FDLE to ensure the reliability, confidentiality, completeness, and accuracy of all records contained in or obtained by means of the CJNet, including the FCIC/NCIC System. The User further acknowledges that failure to comply with these duties and responsibilities will subject its access to various sanctions as approved by the FBI Criminal Justice Information Services Advisory Policy Board. These sanctions may include termination of NCIC services to the User agency. The User may appeal these sanctions through the CSA.
8. **TERM OF AGREEMENT:** This agreement will remain in force until it is determined by FDLE that a new agreement is required. The User Agency should initiate the execution of a new agreement when a change of agency head occurs.

IN WITNESS HEREOF, the parties hereto have caused this agreement to be executed by the proper officers and officials.

NAME OF USER AGENCY _____

AGENCY HEAD

(PLEASE PRINT) TITLE _____

(SIGNATURE)

DATE _____

WITNESS _____ **TITLE** _____

FLORIDA DEPARTMENT OF LAW ENFORCEMENT

BY _____ **TITLE** _____
(PLEASE PRINT)

(SIGNATURE)

DATE _____

WITNESS _____ **TITLE** _____

The User Agreement requires an agency to appoint designated contacts to include the Terminal Agency Coordinator (TAC), Information Security Officer (ISO), CJNet Point of Contact (POC) and FCIC Public Access System (PAS) Contact, if applicable. Please print or type the information. Agency updates should be submitted, preferable on letterhead, to the FDLE within five (5) business days.

FDLE CJIS
Attention: Stephanie Folds
P.O. Box 1489
Tallahassee, FL 32302
Fax 850.410.8188

Contact Information for: _____
(AGENCY)

Terminal Agency Coordinator (TAC)

Name: _____ Title: _____
Phone: _____ Fax: _____
e-mail: _____

Alternate Terminal Agency Coordinator (TAC)

Name: _____ Title: _____
Phone: _____ Fax: _____
e-mail: _____

Information Security Officer (ISO)

Name: _____ Title: _____
Phone: _____ Fax: _____
e-mail: _____

CJNet Point of Contact (POC)

Name: _____ Title: _____
Phone: _____ Fax: _____
e-mail: _____

FCIC Public Access System (PAS) Contact (for entry agencies)

Name: _____ Title: _____
Phone: _____ Fax: _____
e-mail: _____

PAS TIP Information:

PAS TIP Phone: _____

PAS TIP e-mail: _____